Maîtrise des correctifs de sécurité pour les systèmes navals

Type de contenu : Texte

Type de médiation : b

Type de support : Ressource dématérialisée

Titre(s) : Maîtrise des correctifs de sécurité pour les systèmes navals / Bastien Sultan ; sous la direction de Yvon Kermarrec

Auteur(s) : Sultan, Bastien (1992-....)

Autre(s) auteur(s) : Kermarrec, Yvon (1962-....)
Nana Tchamnda, Laurent
Cuppens, Frédéric (1962-....)
El Ouahidi, Bouabid
Brosset, David
Garcia-Alfaro, Joaquin (1976-....)
École nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire
École doctorale Mathématiques et sciences et technologies de l'information et de la communication Rennes
Laboratoire en sciences et techniques de l'information, de la communication et de la connaissance

Production : 2020

Titre traduit ajouté par le catalogueur : Patch management applied to naval systems eng

Autres classifications : 004

Classification décimale Dewey : 004

Note sur le titre et les responsabilités : Titre provenant de l'écran-titre

Note sur la responsabilité : Ecole(s) Doctorale(s) : École doctorale Mathématiques et sciences et technologies de l'information et de la communication (Rennes)
Partenaire(s) de recherche : Lab-STICC_IMTA_CID_IRIS (Laboratoire), Département Logique des Usages, Sciences sociales et Sciences de l'Information (Laboratoire), Laboratoire en sciences et techniques de l'information, de la communication et de la connaissance (Laboratoire)
Autre(s) contribution(s) : Laurent Nana Tchamnda (Président du jury) ; Yvon Kermarrec, David Brosset, Joaquin Garcia-Alfaro (Membre(s) du jury) ; Frédéric Cuppens, Bouabid El Ouahidi (Rapporteur(s))

Note de thèses et écrits académiques : Thèse de doctorat Informatique Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire 2020

Résumé ou extrait : Évoluant dans des environnements contraints et rassemblant dans des espaces réduits des sous-systèmes fortement critiques et hétérogènes, les navires d'aujourd'hui font partie des objets les plus complexes qui soient. À l'heure où croît à leur bord le nombre de systèmes informatiques contrôlant parfois des actionneurs d'importance cruciale, leur maintien en condition de sécurité est une problématique majeure. Les travaux présentés dans cette thèse définissent un processus de gestion des vulnérabilités et des contremesures associées adapté au contexte des systèmes industriels complexes. Ce processus s'appuie sur une méthode et un formalisme de modélisation de ces systèmes permettant d'abstraire leur comportement, discret ou continu, et leurs évolutions éventuelles – apparition d'une vulnérabilité, déploiement d'une contremesure ou survenue d'une attaque – que nous avons définis dans le cadre de ces travaux. Il repose également sur une méthode de calcul des impacts associés aux vulnérabilités, attaques et contremesures aboutissant à leur expression sous la forme d'une métrique adaptée pour la prise de décision. Ce calcul étant permis par la modélisation du système mais aussi par celle des vulnérabilités, attaques et contremesures, nous introduisons par ailleurs une méthode et un formalisme adapté – les mutations d'automates et de réseaux d'automates – permettant leur abstraction. Ces propositions théoriques et méthodologiques sont enfin confrontées à une expérimentation sur un cas fictif représentatif d'un système de propulsion et de gouverne d'un bâtiment de type ferry ou paquebot, permettant de discuter de leur pertinence et de leurs limites ainsi que d'esquisser les perspectives de recherche naissant de nos travaux.
Operating in constrained environments and composed of heterogeneous subsystems, today's ships are among the most complex objects that exist. Due to the increasing number of cyber assets among their components, patch and vulnerability management applied to naval systems is an essential process. The work detailed in this PhD thesis aims to define such a process tailored to complex cyber-physical systems. This process relies on a modelling method and formalism allowing to depict CPS behaviour and cyber events – a vulnerability discovery, a cyber attack occurrence or a patch deployment. It also relies on an impact assessment method, allowing to compute the effects of cyber events on CPS ability to fulfill their missions. These impacts are expressed through a specially designed metric aiming to help in decision-making. The process, methods, formalisms and metrics we propose in this work are then evaluated through an experimentation based on a fictitious case-study.

Configuration requise : Configuration requise : un logiciel capable de lire un fichier au format : text/html ou application/pdf

Sujet(s) : Analyse de risque
Cybersécurité
Vulnérabilités
Correctifs

Sujet - Nom commun : Évaluation du risque
Cyberdéfense
Systémique

Forme, genre ou caractéristiques physiques : Thèses et écrits académiques

Adresse électronique et mode d'accès : http://www.theses.fr/2020IMTA0220/document||Accès au texte intégral de la version partielle
http://www.theses.fr/2020IMTA0220/abes||